Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the	)	WC Docket No. 11-39
Truth in Caller ID Act of 2009	)	

COMMENTS OF ITELLAS LLC

I. Introduction

Itellas LLC ("Itellas" or the "Company") offers these comments on the Commission's proposed regulations to implement the Truth in Caller ID Act of 2009 (the "Truth in Caller ID Act" or the "Act"), signed into law on December 22, 2010.[1]

Itellas owns and operates www.Itellas.com. Through the website, Itellas provides a voice information service (the "Service") that, among other things, allows the caller to spoof a caller ID on a conversation, record the conversation, or alter his or her voice in the conversation. Itellas offers a variety of plans for its Service, ranging from a metered plan at $0.10 per minute, to single user Personal and Business Unlimited plans, and up through scalable plans for larger businesses with greater usage needs. Toll free access (provided through an 800 DID line) costs an additional $14.95 per month.

The Company operates the Service by using open source software along with some modified open source scripts. The software is hosted on a dedicated server owned by Itellas. This dedicated server is the only piece of hardware used to provide the Service. Itellas stores

[1] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

all customer data, billing information, and call logs/records in a secure database, which is kept on a separate server. The Service is used in conjunction with internet-protocol-enabled service from a VOIP service provider that offers real-time, bidirectional voice functionality that mimics traditional voice telephony services.

A customer can place a "spoofed" call through the Service in only one way – by calling the Company's toll free or local dial-in number and entering his personal identification number ("PIN"). Currently, Itellas offers local dial-in numbers only in Birmingham, Boca Raton, Chicago, Los Angeles, and Phoenix. Once the call is connected to the Company's server, the customer enters his desired caller ID and the number he wishes to call, and the call is placed to the called party on the PSTN. The call goes from the Company's dedicated server to the VOIP provider, and then on to the PSTN. Customers may also enable Static Spoofing, a software feature which automatically inserts the same specified Caller ID number for each spoofed call, rather than prompting the caller for a new spoofed number on each call he makes.

II. Issues addressed in the NPRM

a. No Verification or Other Enforcement Duties Should Be Imposed

The Commission correctly did not propose any rules that include any verification, reporting or record keeping requirements. However, paragraphs 12 and 21 of the NPRM invite comment on whether the Commission can and should adopt rules imposing certain obligations on providers of caller ID spoofing services such as Itellas. The NPRM identifies three types of potential requirements that could be imposed on service providers: (1) verification of a user's right to spoof a particular number, (2) record keeping requirements, and (3) reporting requirements.

Narrowly drawn record keeping requirements might be acceptable. However, no rule creating verification or reporting obligations should be imposed. Such a rule would not be legally justified and would not achieve any goals of the Act.

1. The Commission Could Impose Reasonable Record Keeping Requirements

Itellas would not oppose the imposition of reasonable record keeping requirements. However, any record keeping requirement that the Commission might impose should be applied not just to third party service providers, but across the board to all providers of spoofing services, including entities such as businesses running their own Asterisk PBXes and interconnected VOIP providers.

Itellas already retains detailed information about its customers and their use of the Service. Itellas's customers sign up for the service online through www.itellas.com or by purchasing the service via SpoofPro, Itellas's mobile app. Customers use credit cards to pay for the service. Thus, Itellas has relatively complete information about its customers, including, among other data, their name, billing address and credit card number, plus the IP address of the computer from which the purchase was made.[2] Itellas also maintains detailed records of all calls placed through its system, included any call recordings made by that the customer. The software used by Itellas creates a call detail record ("CDR") that contains not only the usual PSTN CDR fields - calling number, ANI, called number, time of call initiation, etc. – but also fields for data such as (i) the spoofed number, (ii) whether the caller changed his or her voice

[2] To ensure that it has this infformation, Itellas does not allow customers to block their caller ID when calling in to use the Service, and it does not allow users to sign up with pre-paid Visa or Master Charge "gift" cards. These steps prevent people from hide their identity and signing up for the Service using a pre-paid phone, in which case Itellas would have no way to confirm who they really are.

using the program's voice change function, (iii) whether the caller recorded the conversation, and several other data points. If the caller did record the conversation, the CDR will also contain a field linking to the recording on Itellas's server.

Itellas's system creates CDRs for each call placed by a customer. Until early 2011, Itellas maintained these CDRs for 180 days. It has now modified its policy and plans to retain CDRs for up to ten years. After ten years, Itellas will allow the logs to be overwritten with new call log data. Any associated call recordings are stored on the server until they are deleted by the customer.

Itellas regularly responds to search warrants, subpoenas, and other forms of valid legal process (collectively, "Subpoenas") from state and federal law enforcement agencies requesting information about the activity of particular accounts. In one of the rare examples Itellas has experienced, one of its customers used the Service to harass a hotel in Lancaster, PA. The hotel asked the police department to place a "trap" on the line so that the next time a prank call was received they could see the ANI in addition to the caller ID. A few days later when another prank call was received and the main Itellas phone number appeared as the ANI, the police knew this was an Itellas customer. Local law enforcement served a subpoena to require Itellas to turn over information about that customer account. As a result of the information provided by Itellas, the police were able to arrest Joy Freeland and stop the calls to the hotel. For more information about this incident, see http://www.wgal.com/r/15375639/detail.html.

On average, Itellas responds to about twenty Subpoenas per year. In addition, Itellas responds to many additional informal requests made through its law enforcement portal at

<http://itellas.com/lookup.php>. That portal allows law enforcement agencies to contact Itellas to determine if it has records showing that its system was used to call or spoof a certain number. If Itellas confirms that it has relevant data, the law enforcement agency can serve a subpoena for the records. Itellas also responds to subpoenas from private parties that call for production of call detail records. Given Itellas's existing capabilities and policies, there would be minimal impact on Itellas if the Commission were to implement regulations requiring detailed record keeping about all customers and their calls.

2. Any Verification Requirement Would be Pointless

The Commission decided not to impose a verification requirement in the NPRM, and it should not do so now.[3] Verification would be pointless and expensive.

Any regulation that required verification would be neither required by nor consistent with the language of the Act. It also would not achieve any goal of the Act. Verification has no relationship to detecting violations of the Act. The Act does not require that a caller using spoofing have the right to use the spoofed number. To put it another way, using a number that you do not have permission to spoof is not illegal under the Act. In fact, the Act's legislative history specifically recognizes that legitimate uses of spoofing may involve situations where the caller is deliberately misleading by hiding his identity, including by using a number which he or she may have no authorization to spoof.[4] Moreover, verification (particularly a single

---

[3] The Department of Justice (DOJ) has urged the Commission to consider adopting rules requiring "public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number." DOJ Jan. 26, 2011 Letter at 4.

[4] For example, Rep. Stearns (R. Tex.) stated in the final House debate on the bill:

> There are sometimes legitimate reasons why someone may need to manipulate caller ID. For example, domestic violence shelters often alter their caller ID information to simply protect the

initial verification of the sort suggested by the DOJ) cannot establish the caller's intent on any spoofed call.

The DOJ has also failed to identify what could or should be done if a caller failed verification. If the caller failed verification, Itellas would have no duty to prevent the call from going through to the called party. Therefore, verifying whether a user has the authority to use the spoofed number would in fact be a pointless exercise.

A verification requirement would unduly burden small entities such as Itellas, which lack the resources to implement such a program. More importantly, it would be nothing more than a thinly disguised attempt to force service providers to do indirectly what neither Congress nor the Commission can do directly – limit the speech of callers by preventing them from spoofing when they have no other criminal intent.

IV. Service Providers Are Already Combating Users' Unlawful Conduct, So New Rules Are Not Necessary

American caller ID spoofing service providers were generally in favor of the Truth in Caller ID Act of 2009, as none of the providers want criminals to sully the industry's reputation as a provider of legitimate business and personal services. Currently, the caller ID replacement/spoofing industry is self-regulated and most responsible service providers have already taken effective steps to address concerns about possible misuse of spoofing. Itellas, for example, takes a variety of strong precautions to prevent criminals from using its

---

safety of victims of violence. Furthermore, a wide array of legitimate uses of caller ID management technologies exists today, and this bill protects those legitimate business practices. Cong. Record H8378 (Dec. 15, 2010).

caller ID replacement service for nefarious purposes. For example, to its knowledge, Itellas has never had a single incident where a customer used its service for swatting. The main reason for this track record is that Itellas' switch has since 2006 been programmed not to allow any customer to call or display 911 through the Service.[5]

Similarly, the Itellas network automatically compares called and spoofed numbers. If a customer chooses to spoof the same number that he is calling, the Itellas system plays a message explaining that hacking someone's voicemail box is strictly prohibited. The system also automatically counts the number of DTMF signals in order to determine if the customer hacked into a voicemail account.[6] Itellas bans for life all customers that hack voicemail boxes. It blacklists them by name, credit card number, and phone number to prevent them from signing back up for the Service.

The Itellas system is also programmed to prevent customers who are calling toll free numbers (e.g., 800 or 866 numbers) from selecting a specific spoofed caller ID, because this could potentially open the door to criminals committing wire fraud and or activating stolen credit cards. Itellas does have a few mystery shoppers as clients, and they need to be able to hide their actual number when calling toll free numbers, so in that situation the Itellas system randomly

---

[5] In response to the question in paragraph 17 of the NPRM, the delivery of caller identification information to E911 public safety answering points should be considered a type of "Caller Identification Service" for purposes of the new rules. The software scripts powering the company's calling card application are set up in such a manner that all calls where the spoofed number is not a ten digit number are blocked. Thus, if a customer were to try to enter "911" as the Caller ID, the call would be blocked.

[6] A DTMF signal is created when the customer pushes a number on the keypad during a call. Itellas has been able to identify the great majority if customers hacking voicemail boxes by flagging any call where the number dialed is the same as the number being spoofed and then counting the number of DTMF tones pushed once the call has been connected. Voicemail hackers typically go back and set voicemails they have heard back to a "new" status so that the real owner of the voicemail box cannot tell that the messages have already been heard by someone else. As a result, such hackers tend to press a lot of buttons in order to listen to voicemails.

picks a 10 digit number to display instead of giving the customer the option to choose a number. This still gives those customers the ability to hide their identities when calling toll free numbers, but since they cannot pick the actual number that is displayed, criminals cannot use Itellas to commit wire fraud or activate stolen credit cards.

In addition, all customers are required to agree to the Itellas Terms of Service (TOS), which state that "Itellas works hand in hand with law enforcement when subpoenaed to ensure that no customer of Itellas is able to use our service to commit crimes, harass, defraud, etc."[7] Itellas also informs its customers that "we keep detailed call logs and reserve the right to monitor any and all use of our service in order to ensure that no customer is using the service in an unlawful manner."[8] This language deters the majority of the potential customers that consider using the Service to commit a crime, as they understand that they are not truly anonymous and Itellas can trace all calls made through their account back to them.

Finally, Itellas cooperates fully with law enforcement and government agencies. Its principals have consulted with the Los Angeles Police Department, the Department of Homeland Security, and various other government agencies when they have contacted Itellas seeking information on how the spoofing process works.

Itellas believes that the best approach for the Commission to take would be to recommend that all entities providing caller ID spoofing capability adopt the types of best practices that Itellas already follows. By simply encouraging providers to keep detailed call logs and customer information, the Commission could ensure that many criminals who use Itellas or

---

[7] See http://www.itellas.com/tos.php.

[8] Id.

other American commercial call spoofing providers to commit crimes could be identified and prosecuted. The quickest and most economical solution would be to foster an informal partnership between the private sector and law enforcement, as opposed to over- regulating and possibly eliminating a profitable private sector service that pays taxes. The increased administrative and technical burdens that would result from creating strict regulations, such as requiring customers to prove that they have the right to use the number(s) they are displaying on the caller ID, would only serve to increase costs and shut down legitimate spoofing companies. Those customers that use spoofing in unethical ways would just find other means to accomplish their goals. These "other means" most likely would not provide any way to trace the calls back to an individual, so there would be no evidence that law enforcement could use to bring perpetrators to justice.

V. Service Providers Should Be Exempt From Liability For Their Users' Spoofing

The Commission also seeks comment on whether it should "more generally exempt conduct by carriers or interconnected VoIP providers that is necessary to provide services to their customers." *Id.*, para. 23. The answer is yes. The Act gives the Commission the authority to adopt additional exemptions to the prohibition on using caller ID spoofing if it determines them to be appropriate.[9] The Commission should exercise this authority by modifying Section 64.1604(b) to make clear that *any provider of spoofing services* – whether a common carrier, an interconnected VoIP provider or an information services provider such as Itellas - is exempt from

[9] *Id.* § 227(e)(3)(B)(i).

liability under the Act unless the service provider itself has the necessary intent to defraud, cause harm or wrongfully obtain anything of value. The service provider ordinarily has no way of knowing whether or not the caller has "the intent to defraud, cause harm or wrongfully obtain anything of value," so the service provider itself ordinarily cannot have such intent and thus cannot be in violation of the Act. Absent such intent, a "carrier or provider merely transmits the caller ID information it receives from another carrier, provider, or customer" (NPRM at para. 23) and cannot violate the Truth in Caller ID Act.

Congress did not create liability for service providers – whether carriers, interconnected VOIP providers, information service providers such as Itellas, or businesses operating PBXes - that are merely transmitting information selected by a caller. The Commission's rules should make this clear. Such an explicit expression will prevent confusion and help small businesses such as Itellas by minimizing unnecessary litigation and expense down the road.

Conclusion

The proposed rules should be adopted (subject to being amended as suggested above) and applied to all providers of caller ID spoofing services.

Respectfully submitted,

_____/s/_____

Mark C. Del Bianco
Counsel for Itellas
Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
Tel: 301-933-7216
mark@markdelbianco.com

Date: April 18, 2011

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 18th day of April, 2011, a true and correct copy of the foregoing Comments was served electronically on the following:

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
(**via ECFS filing**)

Best Copy and Printing, Inc.
Portals II
445 12th Street, S.W.
Room CY-B402
Washington, DC 20554
fcc@bcpiweb.com

Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington D.C. 20554
cpdcopies@fcc.gov

___/s/_____
Mark C. Del Bianco